

RECEIVED  
CENTRAL FAX CENTER

NOV 02 2005

ATTORNEYS AT LAW

## USPTO FACSIMILE TRANSMITTAL SHEET

TO:	FROM:		
Examiner Christian A. LaForgia			
ORGANIZATION:	Matthew W. Baca, Reg. No. 42,277		
ART UNIT:	CONFIRMATION NO.:	DATE:	
2131		November 2, 2005	
FAX NUMBER:	TOTAL NO. OF PAGES INCLUDING COVER:		
571.273.8300	8		
ENCLOSED:	APPLICATION SERIAL NO.:		
Reply Brief	09/696,518		
	ATTORNEY DOCKET NO.:		
	FR919990110US1		

URGENT  FOR REVIEW  PLEASE COMMENT  PLEASE REPLY  PLEASE RECYCLE

## NOTES/COMMENTS:

CERTIFICATE OF FACSIMILE TRANSMISSION UNDER 37 C.F.R. § 1.8(a)

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING FACSIMILE TRANSMITTED TO THE U.S. PATENT AND TRADEMARK OFFICE ON NOVEMBER 2, 2005.

SIGNATURE OF MICHELLE SANDERSON

A handwritten signature in black ink, appearing to read "Michelle Sanderson".

This fax from the law firm of Dillon & Yudell LLP contains information that is confidential or privileged, or both. This information is intended only for the use of the individual or entity named on this fax cover letter. Any disclosure, copying, distribution or use of this information by any person other than the intended recipient is prohibited. If you have received this fax in error, please notify us by telephone immediately at 512.343.6116 so that we can arrange for the retrieval of the transmitted documents at no cost to you.

8911 N. CAPITAL OF TEXAS HWY., SUITE 2110, AUSTIN, TEXAS 78759  
512.343.6116 (V) • 512.343.6446 (F) • DILLONYUDELL.COM

RECEIVED  
CENTRAL FAX CENTER

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

NOV 02 2005

IN RE APPLICATION OF:

DOCKET NO.: FR919990110US1

OLIVIER DAUDE

EXAMINER: CHRISTIAN A. LA FORGIA

SERIAL No.: 09/696,518

ART UNIT: 2131

FILED: OCTOBER 25, 2000

FOR: M/S FOR PREVENTING  
UNAUTHORIZED SERVER  
INTERFERENCE IN AN INTERNET  
PROTOCOL NETWORKREPLY BRIEF UNDER 37 C.F.R. 41.41Mail Stop Briefs - Patents  
Commissioner for Patents  
Washington, D.C. 20231

Sir:

This Reply Brief is submitted in response to Examiner's Answer dated September 7, 2005. No fee is believed to be required to submit this Reply Brief. However, in the event any fees are required, please charge IBM CORPORATION'S Deposit Account No. 09-0457. No extension of time is believed to be necessary. However, in the event an extension of time is required, that extension of time is hereby requested. Please charge any fee associated with an extension of time as well as any other fee necessary to further the prosecution of this application to IBM CORPORATION'S Deposit Account No. 09-0457.

Certificate of Transmission/Mailing

I hereby certify that this correspondence is being facsimile transmitted to the USPTO at 571-273-8300 or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:  
Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on the date shown below.

Typed or Printed Name: Michelle Sanderson Date: November 2, 2005 Signature: MSanderson

REMARKS

In the Response to Argument, on page 3, the Examiner's Answer traverses Appellants' position that "Authentication of DHCP Messages" to Droms et al. (hereinafter *Droms*), fails to disclose "detecting an unauthorized dynamic host configuration server ... in accordance with server identification data within the configuration offer messages." Supporting this traversal, the Answer describes the shared-token approach of "Protocol 0" with no discussion of the manner in which "server identification data" is used in the authentication process. The Answer also alludes to "Protocol 1," explaining "... the server replies with a DHCPOFFER message that includes authentication information, including entity authentication information." Appellants agree that both *Droms*'s Protocol 0 and Protocol 1 utilize authentication information in the offer message to authenticate or "authorize" the server. Appellants urge, however, that the "server identification data" feature expressly added by Amendment, while arguably a subset of, is clearly not an equivalent in scope to, "authentication data" in general. Information used to authorize or authenticate *may or may not* include information that identifies an entity. *Droms*'s disclosure makes it clear that neither Protocol 0 nor Protocol 1 utilize server identification data for authentication purposes. "Protocol 1" uses an encrypted message authentication code and not server identification data to authenticate the server as well as authenticating the message. (See *Droms* paragraph 4, page 4, explaining, "... the client requests authentication in its DHCPDISCOVER message and the server replies with a DHCPOFFER message that includes authentication information. This authentication information contains an encrypted value generated by the source as a message authentication code (MAC) to provide message authentication and entity authentication." (Emphasis added). "Protocol 0" depicted in section 3, pg. 3- pg. 4, utilizes an "opaque, unencoded" authentication token that is known (i.e. pre-specified) to both the client and server and that provides mutual authentication. *Droms*'s disclosure provides no indication that the token contains data that identifies either the client or server.

In Amendment A, Appellants specified "server identification data" as the particular type of data used to authorize the DHCP server consistent with the aim of the invention to provide a one-sided checker client functionality that can be plugged into a DHCP system without having to alter the legacy DHCP system. Appellants' use of server identification data is in contrast to the

REPLY BRIEF  
Docket No. FR9-1999-0110US1  
Page 2 of 7

authentication data used in both *Droms's* Protocol 0 and Protocol 1 that each require two-sided (client and server) compatibility.

With continued reference to the "server identification data" feature, Appellants agree that prior art DHCPOFFER messages may include data, such as an IP address, that may be reasonably interpreted as "server identification data." Appellants contend, however, that the inclusion of server identification data in the DHCPOFFER message does not compel a conclusion, as suggested by the Answer, that said server identification data is necessarily utilized for server authentication. An example of a non-authentication use of the IP address is that it may be used to provide the recipient client the means to establish communications with the offering server. As explained above, *Droms's* disclosure indicates that neither the "Protocol 0" nor the "Protocol 1" technique utilizes an IP address or any other server identification data to authenticate the offering server.

Relating to the same claim element, the Answer mischaracterizes Appellants' contentions relating to the rejections of the claims. Specifically, the Answer asserts that Appellants' arguments rely on the server identification data being an IP address. In fact, Appellants undertake no such reliance and instead, referring to page 7 of the Appeal Brief, allude to the support in the Specification providing an exemplary characterization of "server identification data," which must be construed most broadly consistent with the Specification. The Answer points out that the prior art references disclose that DHCP messages includes the sender's IP address. Appellants agree that supplying server identification data, in the form of an IP address or otherwise, is known and inherent in disclosures relating to DHCP messages as well as most other IP traffic. However, Appellants again urge that the presence of server identification data in a DHCP offer message does not compel an inference that this data is utilized in any particular authentication routine such as the "Protocol 0" or "Protocol 1" routines disclosed by *Droms*.

On page 4, the Examiner's Answer again mischaracterizes Appellants' contentions regarding the claim elements, asserting Appellants rely on a "server checker client" not mentioned in the claim language, and implying that Appellants have improperly limited such a client to being hardware rather than a program. Appellants have undertaken no unwarranted reliance nor have limited the meaning of "server checker client" to hardware rather than program instructions. Appellants do not rely on the label "server checker client" per se. Instead, and as

REPLY BRIEF  
Docket No. FR9-1999-0110US1  
Page 3 of 7

clearly explained on page 8 of the Appeal Brief, the functional characterization imputed to the “server checker client” (described broadly therein by Appellants as a “logical entity”) is required by the claim language. Namely, the logical entity, referred to as the “server checker client,” that unicasts configurations requests to disable the detected unauthorized DHC server from responding to configuration requests from network clients is the same client (logically but not necessarily physically distinct) that performs the broadcasting, receiving, and detecting steps as expressly required by the preceding claim elements. The characterization of the server checker client as the logical entity that performs the broadcasting, receiving, and detecting steps is a substantive and significant characterization of the “unicasting” step given that, Appellants invention is designed to employ a logically (and possibly physically) discrete server checker client such that the legacy DHCP network components and protocols may remain unchanged.

While claims terms must be given their broadest reasonable interpretation consistent with the specification, the Answer’s definition of “server checker client” as being “merely a program running on a workstation” improperly deviates from the express and unambiguous claim language itself.

The fourth element of Claim 1 (and similarly for Claims 14 and 27) recites, in part, “responsive to said detecting step, unicasting host configuration requests from said server checker client to said unauthorized dynamic configuration server...” In addition to the foregoing misinterpretation of the server checker client as meaning *any* client or workstation, on pages 4 and 5, the Answer fails to properly address at least two key limitations in this element. First, Appellants have repeatedly urged that the express limitation that the unicasting step be performed in response to detecting the unauthorized DHC server is a key feature that is absent from any of the cited references either individually or in combination.

On page 5, the Answer defines “unicasting” and proceeds to incorrectly conclude that U.S. Pat. No. 5,884,024, issued to Lim (hereinafter *Lim*) discloses unicasting host configuration requests from the client to the unauthorized DHCP server. Also on page 5, the Answer further incorrectly asserts that *Lim* states that using a single client to obtain all IP address leases from a DHCP server, other clients are blocked from access to the IP addresses, thereby preventing clients from receiving false configuration information and becoming victims of denial of service or man in the middle attacks. In fact, *Lim* describes an “IP address hogging attack” by one client

REPLY BRIEF  
Docket No. FR9-1999-0110US1  
Page 4 of 7

against one or more other clients and does not state anything about any potentially beneficial ramification, whether it be silencing an unauthorized server or otherwise, of such an "attack." Rather than teaching unicasting configuration requests to "silence" an unauthorized server, *Lim's* non-express but arguably inherent disclosure of unicasting host configuration requests to a server covers only the incidental and contextually undesired disabling of a DHCP server resulting from the IP address hogging. The disclosure of *Droms* is limited to authentication/authorization and contains no disclosure or suggestion whatsoever relating to any method for disabling a server found to be unauthorized. Neither *Droms* nor *Lim*, individually or in combination, relate to deliberately disabling DHCP servers and therefore neither provides a suggestion or motivation to combine what is described as a client-to-client attack by *Lim* as a response to detecting a non-authenticated DHCP server as shown in *Droms*.

The second limitation of the foregoing unicasting element not properly addressed by the Answer again relates to the characterization of the "server checker client" as being the same logical entity that performs the broadcasting, receiving, and detecting steps as explained above.

On page 6, the Answer appears to shift the grounds for rejecting claims 8, 21, and 34 from *Droms* to disclosure by *Lim*, and incorrectly asserts that Appellants' arguments for overcoming the prior art rely on the absence of disclosure of a "server table." The Claim element in question recites, in part, "wherein said checker client includes a server table having a list of authorized dynamic host configuration servers, and wherein said step of detecting an unauthorized dynamic host configuration server further comprises comparing a server identifier included in each configuration offer message with authorized server identification data in the server table." Appellants agree that in FIG. 6 and col. 6, line 55 through col. 7, line 20, *Lim* discloses a trusted identifier database 318. Appellants note, however, that database 318 does not maintain any list of authorized DHCP servers. Instead, as explained at col. 6, lines 2-6, col. 7, lines 9-14 and lines 31-39, the "trusted identifiers" maintained by database 318 are data objects that identify a relay agent (e.g. cable modems) associated with a single client system. Appellants further note that none of the references, either individually or in any combination, disclose "comparing a server identifier included in each configuration offer message with authorized server identification data in the server table" to detect an unauthorized server.

REPLY BRIEF  
Docket No. FR9-1999-0110US1  
Page 5 of 7

Appellants have clearly shown that the combination of *Daizo*, *Droms*, and *Lim* neither contemplates nor suggests the proposed invention recited in Appellants' claims, and for those reasons, Examiner's rejection of Appellants' claims is not well founded and should be reversed.

REPLY BRIEF  
Docket No. FR9-1999-0110US1  
Page 6 of 7

CONCLUSION

Appellants have again pointed out with specificity the manifest error in the Examiner's rejections, and the claim language which renders the invention patentable over the reference. Appellants, therefore, respectfully request that the present rejections be reversed.

Respectfully submitted,

  
Matthew W. Baca  
Reg. No. 42,277  
Dillon & Yudell LLP  
8911 North Capital of Texas Highway  
Suite 2110  
Austin, Texas 78759  
512.343.6116

ATTORNEY FOR APPELLANTS

REPLY BRIEF  
Docket No. FR9-1999-0110US1  
Page 7 of 7